UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,121	04/27/2001	Bjorn Markus Jakobsson	45-1-1	1053

7590 12/06/2005

Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 12/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/844,121	JAKOBSSON ET AL.	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 September 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on September 16, 2005. Claims 1-28 were originally received for consideration. Claims 1,15,27, and 28 are amended per the received amendment. Claims 1-28 are currently being considered.

Response to Arguments

2. Applicant's arguments filed September 16, 2005 have been fully considered but they are not persuasive for the following reasons:

Regarding claim 1, the applicant argues that the cited prior art (CPA), Walker et. al (U.S. Patent 6,257,638), does not teach the limitations of initiating an interaction between two processing devices by sending "designated initiation information to the second processing device..., the particular interaction being configured based at least on part on one or more results from a setup procedure." This argument is not found persuasive. The CPA discloses "a handshake recognition sequence, the verification of the player's identity with the wagering establishment" (column 13 lines 53-55). This handshake is initiated when the player (first processing device) calls the wagering establishment either on the phone or through on-line means (column 7 lines 1-8) and the player (first processing device) establishes his/her identity by way of a personal

identification message and software identification message (column 13 lines 57-62). Furthermore, the applicant argues that the CPA does not teach sending additional information to a second processing device "based at least in part on the received response information." This argument is not found persuasive. After the initiation step is completed, the wagering establishment (second processing device) sends an authenticable handshake message to the player (first processing device) which the player can authenticate, which is only possible if the handshake message is related to the player's identity, and subsequently, the player produces an authenticable recognition response message which is provided back to the wagering establishment (second processing device) (column 13 line 60 – column 14 line 7). Furthermore, the applicant argues that the CPA does not teach "wherein the interaction is configured such that the information exchanged between the first and second processing devices can be used to determine rights of the first and second participants in a publicly verifiable manner." This argument is not found persuasive. The information exchanged by the two processing devices can be interpreted to include wagers, specific lottery numbers, and the amount of money won/lost. Therefore, the CPA discloses the player's choice of wagering elements (i.e. numbers) are presented in an authenticable message include a data/time stamp, the player's identification code, and the computer/software identification code (column 4 lines 10-21), which are verifiable to prove the validity of the user's claims. Furthermore, the audit trail which provides a record of all activities taking place between the first and second processing devices (i.e. the gaming computer and the wagering establishment) (column 6 lines 20-33). Regarding dependent claim 6, the

applicant argues that the CPA does not disclose "two or more players." This argument is not found persuasive. The CPA disclose that the game being played can be blackjack, which is between at least 2 players (the dealer and the player) (column 8 lines 55-63). Regarding claim 9, the applicant argues that the CPA does not teach a "symmetric cipher... having a semantic security operating in conjunction with a one-way hash function." The CPA discloses that the authenticable messages can use encryption, digital signatures, one-way hashes, checksums and the like (column 6 lines 1-7). Regarding claim 10, the applicant argues that the configuration of the interaction cannot handle a disconnection of the parties. The CPA discloses that the "financial resolution of each wager is cumulatively tracked by the software on the gaming computer and perhaps also on any networked computers, so that the player is able to constantly monitor his or her gambling credit balance with the wagering establishment" (column 6 lines 50-54). This cumulative tracking provides insurance so that if the connection is lost, the player is insured that the balance was what it was at the last point before disconnection. Regarding claim 12, the applicant argues that the CPA does not teach a "tree structure." The CPA states that the game can be roulette, which has a random outcome on each round of the game, and can provide results for colors, even, odds, blocks of numbers, or individual numbers. Therefore, it is respectfully asserted that the CPA does teach the above limitations and the rejection for the claims is respectfully maintained as given below.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-6, 8-12, 14-20, and 22-28 rejected under 35 U.S.C. 102(e) as being anticipated by Walker et al. (U.S. Patent No. 6,257,638).

Regarding claim 1, Walker discloses:

A method for performing secure information processing operations utilizing a plurality of processing devices, the method comprising the steps of:

performing a setup procedure to permit interactions of a designated type to be carried out between a first participant associated with at least a first one of the processing devices and a second participant associated with at least a second one of the processing devices (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

initiating in the first processing device a particular interaction with the second participant, by sending designated initiation information to the second processing device

associated with the second participant, the particular interaction being configured based at least in part on one or more results of the setup procedure (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

receiving as part of the interaction response information from the second processing device associated with the second participant (column 5 line 56 – column 6 line 20); and

sending as part of the interaction additional information from the first processing device to the second processing device based at least in part on the received response information (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

wherein the interaction is configured such that the information exchanged between the first and second processing devices can be used to determine rights of the first and second participants in a publicly verifiable manner, the rights being based upon particular results of the interaction (column 4 lines 10-22, column 6 lines 21-54).

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Walker discloses:

The method of claim 1 wherein the receiving and sending steps are repeated one or more times in accordance with specifications of the particular interaction (column 10 lines 42-46, column 13 lines 25-38, column 13 line 43 – column 14 line 7).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Walker discloses:

The method of claim 1 wherein the first processing device comprises at least one lightweight device configured to communicate over a network with the second processing device (column 8 lines 33-40).

Claim 4 is rejected as applied above in rejecting claim 1. Furthermore, Walker discloses:

The method of claim 1 wherein the particular interaction comprises secure mobile gaming interaction in which the first participant corresponds to a player and the second participant corresponds to a casino (column 8 lines 23-33).

Claim 5 is rejected as applied above in rejecting claim 4. Furthermore, Walker discloses:

The method of claim 4 wherein the first processing device comprises a lightweight processing device associated with the player and the second processing device comprises at least one server associated with the casino (column 8 lines 23-47)

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Walker discloses:

The method of claim 1 wherein the particular interaction comprises secure mobile gaming interaction involving two or more players in which the first participant

corresponds to a first player and the second participant corresponds to a second player (column 8 lines 23-47, column 11 lines 38-50).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Walker discloses:

The method of claim 1 wherein the particular interaction comprises secure digital signature exchange interaction in which the first participant corresponds to a first party to the digital signature exchange and the second participant corresponds to a second party to the digital signature exchange (column 5 line 56 – column 6 line 20)

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Walker discloses:

The method of claim 1 wherein security of the particular interaction is based at least in part on a secure probabilistic symmetric cipher (E, D) having semantic security operating in conjunction with a one-way hash function h for which collisions are intractable to find, and a commitment function C, wherein the commitment function C provides the public verifiability of designated portions of the interaction (column 5 line 56 – column 6 line 20).

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Walker discloses:

The method of claim 1 wherein the interaction is configured such that if at least one of the first and second processing devices is disconnected during the interaction, the interaction may upon reconnection of the device be continued from a designated point at or prior to the disconnection without the participants being able to alter any partial results of the interaction attributable to a portion of the interaction up to the designated point (column 4 lines 10-21, column 6 lines 43-54).

Claim 11 is rejected as applied above in rejecting claim 4. Furthermore, Walker discloses:

The method of claim 4 wherein the secure mobile gaming interaction comprises at least one game played by the player with the casino, the game comprising a number of consecutive rounds of one or more moves by each of the player and the casino, each of the rounds allowing the player and the casino to commit to at least one decision (column 11 lines 38-50, column 15 lines 29-53).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Walker discloses:

The method of claim 11 wherein the game is characterized by a player game tree structure associated with the player and a casino game tree structure associated with the casino, each of the game tree structures comprising a plurality of nodes, each of at least a subset of the nodes comprising a block of data that determines randomness contributed to a corresponding round of the game by the corresponding player or

casino, wherein associated with each of at least a subset of the game nodes are decision preimage values that encode possible decisions to be made in the game (column 11 lines 8-30).

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Walker discloses:

The method of claim 12 wherein the setup procedure comprises at least the following steps:

(a) the player selecting n random numbers d.sub.il, . . . , d.sub.in, for each node i of the player game tree structure, and a random number r.sub.i uniformly at random for each node, wherein each node i corresponds to a particular round of the game;

(b) the player computing for each node i a corresponding game node value game.sub.i=<h(D.sub.il, . . . D.sub.in), R.sub.i>, where D.sub.ij=h(d.sub.ij), R.sub.i=C(r.sub.i), h denotes a hash function, C denotes a commitment function, and preimage.sub.i=(d.sub.il, . . . , d.sub.in, r.sub.i,) denotes a decision preimage value for game.sub.i;

(c) the player computing for each node i a value which is a function of one or more of: (i) values associated with one or more of its children nodes; (ii) its corresponding game node value game.sub.1; and (iii) a descriptor that identifies the game type;

(d) both the player and the casino storing information of the form agreement .sub.(casino,player) comprising a root value of the player game tree structure, a root

value of the casino game tree structure, a hash value on a game function .function..sub.game, and associated digital signatures by the player and the casino.

Claim 14 is rejected as applied above in rejecting claim 12. Furthermore, Walker discloses:

The method of claim 12 wherein the secure mobile gaming interactions are implemented in accordance with a game-playing protocol comprising at least the following steps:

(a) the player initiating the game by sending a value r.sub.player,cnt the casino, where cnt corresponds to a counter (column 12 line 56 – column 13 line 38));

(b) the casino verifying that r.sub.player,cnt is a correct preimage to R.sub.player,cnt , and halting the protocol if it is not the correct preimage (column 11 lines 8-30, column 12 line 56 – column 13 line 38);

(c) the casino and the player taking turns making moves in which the casino sends to the player decision preimages encoding its move, the player is presented with one or more corresponding choices via an interface at the first processing device, and a given choice selected by the player is translated into one or more preimages that are subsequently sent to the casino (column 11 lines 8-30, column 15 lines 39-64);

(d) step (c) being repeated one or more times in accordance with the rules of the game (column 15 lines 39-64);

(e) the casino sending a value r.sub.casino,cnt to the player, which is verified correspondingly by the player (column 6 line 43 – column 7 line 23);

(f) evaluating a game function .function..sub.game on the disclosed portions of the player and casino preimages, presenting a corresponding output to the player and the casino, and sending appropriate payment transcripts to at least one financial institution (column 7 lines 23-35); and

(g) the player and the casino each updating the counter cnt, along with other state information associated with a current state of the game (column 6 line 43 – column 7 line 23).

Regarding claim 15, Walker discloses:

An apparatus for use in performing secure information processing operations, the apparatus comprising:

a memory (column 2 lines 32-39); and

a processor coupled to the memory, the memory and processor being elements of a first processing device associated with a first participant, the processor being operative:

(i) to perform a setup procedure to permit interactions of a designated type to be carried out between the first participant and a second participant associated with at least a second processing device (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

(ii) to initiate a particular interaction with the second participant, by sending designated initiation information to the second processing device associated with the second participant, the particular interaction being configured based at least in part on

one or more results of the setup procedure (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

(iii) receiving as part of the interaction response information from the second processing device associated with the second participant (column 5 line 56 – column 6 line 20); and

(iv) sending as part of the interaction additional information from the first processing device to the second processing device based at least in part on the received response information (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

wherein the interaction is configured such that the information exchanged between the first and second processing devices can be used to determine rights of the first and second participants in a publicly verifiable manner, the rights being based upon particular results of the interaction (column 4 lines 10-22, column 6 lines 21-54).

Regarding claim 27, Walker discloses:

An article of manufacture comprising a machine-readable storage medium for storing one or more programs for use in performing secure information processing operations utilizing a plurality of processing devices, wherein the one or more programs when executed implement the steps of:

performing a setup procedure to permit interactions of a designated type to be carried out between a first participant associated with at least a first one of the processing devices and a second participant associated with at least a second one of

the processing devices (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

initiating in the first processing device a particular interaction with the second participant, by sending designated initiation information to the second processing device associated with the second participant, the particular interaction being configured based at least in part on one or more results of the setup procedure (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

receiving as part of the interaction response information from the second processing device associated with the second participant (column 5 line 56 – column 6 line 20); and

sending as part of the interaction additional information from the first processing device to the second processing device based at least in part on the received response information (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

wherein the interaction is configured such that the information exchanged between the first and second processing devices can be used to determine rights of the first and second participants in a publicly verifiable manner, the rights being based upon particular results of the interaction (column 4 lines 10-22, column 6 lines 21-54).

Regarding claim 28, Walker discloses:

A method for performing secure information processing operations utilizing a plurality of processing devices including at least a first processing device associated

with a first participant and a second processing device associated with a second participant, the method comprising the steps of:

receiving from the first processing device in the second processing device designated initiation information initiating a particular interaction between the first participant and the second participant, the particular interaction being configured based at least in part on one or more results of a setup procedure, the setup procedure being performed by the first participant associated with the first processing device and permitting the particular interactions to be carried out between the first participant and the second participant (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10);

sending as part of the interaction response information from the second processing device associated with the second participant (column 5 line 56 – column 6 line 20, column 9 lines 41-59, column 12 line 56 – column 13 line 10); and

receiving as part of the interaction additional information sent from the first processing device to the second processing device based at least in part on the response information (column 5 line 56 – column 6 line 20);

wherein the interaction is configured such that the information exchanged between the first and second processing devices can be used to determine rights of the first and second participants in a publicly verifiable manner, the rights being based upon particular results of the interaction (column 4 lines 10-22, column 6 lines 21-54).

4. Claims 16-20, and 22-26 are apparatus claims analogous to the method claims 1-6, 8-12, and 14 rejected above, and therefore, are rejected following the same reasoning.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 7, 13, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Walker et al. (U.S. Patent No. 6,527,638) in view of Takaragi et al. (U.S. Patent No. 5,018,196).

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Walker discloses:

The method of claim 1. Walker does not explicitly disclose that the particular interaction comprises secure contract signing interaction in which the first participant corresponds to a first party to the contract and the second participant corresponds to a second party to the contract. Takaragi discloses a system wherein two parties exchange preliminary digital signatures, and then agree to a contract by exchanging their formal digital signatures with each other, and further, if there are problems, a third party can decode the signatures submitted by the transaction parties, and use a hash total of the

contract, to verify the transaction (Abstract, column 4 lines 14-47). Walker and Takaragi are analogous arts in that both exchange authenticable messages with digital signatures. Walker disclose a system of cashing out, purchasing more gambling credit, via a communication with the wagering establishment (casino). This procedure requires the exchange of authenticable messages as disclosed by Walker. It would have been obvious that these authenticable messages could compose of a contract which has to be digitally signed by each party. This would allow a third party to intervene if a problem arises, so that "neither of the transacting parties can deny that it has approved formally the transaction, if the other party submits its digital signature as evidence" (column 5 lines 7-14). This would be important in the transactions involved in Walker which involve monetary funds. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the contract signing method of Takaragi with the system of verifying the exchange of funds of Walker, to insure the liability of both parties when exchanging monetary funds.

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Walker discloses:

The method of claim 12 wherein the setup procedure comprises at least the following steps:

(a) the player selecting n random numbers d.sub.il, . . . , d.sub.in, for each node i of the player game tree structure, and a random number r.sub.i uniformly at random for

each node, wherein each node i corresponds to a particular round of the game (column 15 lines 39-64);

(b) the player computing for each node i a corresponding game node value game.sub.i=<h(D.sub.il, . . . D.sub.in), R.sub.i>, where D.sub.ij=h(d.sub.ij), R.sub.i=C(r.sub.i), h denotes a hash function, C denotes a commitment function, and preimage.sub.i=(d.sub.il, . . . , d.sub.in, r.sub.i,) denotes a decision preimage value for game.sub.i (column 5 line 56 – column 6 line 20, column 11 lines 10-30);

(c) the player computing for each node i a value which is a function of one or more of: (i) values associated with one or more of its children nodes; (ii) its corresponding game node value game.sub.1; and (iii) a descriptor that identifies the game type (column 5 line 56 – column 6 line 20, column 11 lines 10-30);

Walker does not explicitly disclose that the player and the casino store an agreement (casino, player) comprising a root value of the player game tree structure, a root value of the casino game tree structure, a hash value on a game function, and associated digital signatures by the player and the casino. Takaragi discloses a system wherein two parties exchange preliminary digital signatures, and then agree to a contract by exchanging their formal digital signatures with each other, and further, if there are problems, a third party can decode the signatures submitted by the transaction parties, and use a hash total of the contract, to verify the transaction (Abstract, column 4 lines 14-47). Walker and Takaragi are analogous arts in that both exchange authenticable messages with digital signatures. Walker disclose a system of

cashing out, purchasing more gambling credit, via a communication with the wagering establishment (casino). This procedure requires the exchange of authenticable messages as disclosed by Walker. It would have been obvious that these authenticable messages could compose of a contract, which has to be digitally signed by each party. This would allow a third party to intervene if a problem arises, so that "neither of the transacting parties can deny that it has approved formally the transaction, if the other party submits its digital signature as evidence" (column 5 lines 7-14). This would be important in the transactions involved in Walker which involve monetary funds. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the contract signing method of Takaragi with the system of verifying the exchange of funds of Walker, to insure the liability of both parties when exchanging monetary funds.

6. Claim 21 is an apparatus claim analogous to the method claim of claim 13, and therefore, is rejected following the same reasoning.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Primary Examiner
AU2131
12.1.05

KA
11/28/2005